

Docket No.: 062807-0040



PATENT

AP 27u

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of	:	Customer Number: 20277
Yoko KUMAGAI, et al.	:	Confirmation Number: 9550
Application No.: 10/076,624	:	Tech Center Art Unit: 2131
Filed: February 19, 2002	:	Examiner: Trang T. Doan
For: PUBLIC KEY CERTIFICATE GENERATION METHOD, VALIDATION METHOD AND APPARATUS THEREOF		

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief in support of the Notice of Appeal filed August 2, 2006. Please charge the Appeal Brief fee of \$500.00 to Deposit Account 500417.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. 1.17 and 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Gene Z. Robinson

Registration No. 33,351

**Please recognize our Customer No. 20277
as our correspondence address.**

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 GZR:lnm
Facsimile: 202.756.8087
Date: September 28, 2006



TABLE OF CONTENTS

Page

I.	REAL PARTY IN INTEREST.....	2
II.	RELATED APPEALS AND INTERFERENCES	2
III.	STATUS OF CLAIMS	2
IV.	STATUS OF AMENDMENTS	3
V.	SUMMARY OF INVENTION.....	3
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL	4
VII.	ARGUMENT.....	4
VIII.	CLAIMS APPENDIX	10
IX.	EVIDENCE APPENDIX.....	13
X.	RELATED PROCEEDINGS APPENDIX.....	14

09/29/2006 MAHMEI 00000075 500417 10076624
01 FC:1402 500.00 DA

Application No.:

Docket No.: 062807-0040



PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of	:	Customer Number: 20277
Yoko KUMAGAI, et al.	:	Confirmation Number: 9550
Application No.: 10/076,624	:	Tech Center Art Unit: 2131
Filed: February 19, 2002	:	Examiner: Trang T. Doan
For: PUBLIC KEY CERTIFICATE GENERATION METHOD, VALIDATION METHOD AND APPARATUS THEREOF		

APPEAL BRIEF

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal of the final rejection of claims 11 through 20, filed August 2, 2006.

I. REAL PARTY IN INTEREST

This application is assigned to Hitachi, Ltd.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 11 through 20 are pending and stand rejected as stated in the final Office Action (hereinafter "the Office Action") dated March 28, 2006. Claims 11 through 20 are presented in Claim Appendix VIII supra. Claims 1 through 10 have been cancelled.



IV. STATUS OF AMENDMENTS

No amendment has been filed subsequent to the date of the final Office Action. An interview was conducted on July 12, 2006. An agenda for the interview, as required by the Examiner, was filed June 29, 2006. The Examiner's Interview Summary of the interview is dated July 7, 2006. A Pre-Appeal Brief Request for Review was submitted August 2, 2006. A Notice of Panel Decision from Pre-Appeal Brief Review, issued August 30, 2006, states that there is at least one issue for appeal but is silent as to whether any issues have been resolved.

V. SUMMARY OF INVENTION

The invention is related to encryption technology, particularly to a public key certificate issuing technique and a technique for verifying the validity of the public key certificate in the public key infrastructure (PKI). A method is provided for generating a certificate, and validating or invalidating the certificate. Information assured by a registration authority is written in a certificate issued by an issuing authority. A signature of the registration authority is then applied to the information assured by the registration authority, thereby clearly indicating that the registration authority assures the information for a user who uses the certificate. A public key certificate issuing operation is described in the specification with respect to the flowchart of Fig. 6.

Fig. 9 and its corresponding description in the specification at pages 22-24, describe guaranteeing information 93 by the registration authority RA by using a signature object identifier. This information includes: a name 111 of the registration authority RA; the signature object identifier 112 specifying the information guaranteed by the registration authority RA; and a signature 113 of the registration authority generated by the secret key of the registration authority RA. The signature object identifier 112 specifies the information to be described in the public key certificate among the information checked and examined by the registration authority in step S1004 of the flowchart of Fig.

6. Information to be guaranteed by the registration authority RA includes, for example, the end entity name (subject name), the public key and attribute information of the end entity EE. The registration authority RA generates a signature for the information specified by this identifier (RA signature 113).

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

A. Claim 12 stands rejected under the second paragraph of 35 U.S.C. § 112.

B. Claims 11 through 20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. patent 6,990,583 (hereinafter “Matsuyama”).

VII. ARGUMENT

A. The rejection of claim 12 under the second paragraph of 35 U.S.C. § 112.

The statement of this rejection is presented at paragraphs 4 and 5 (page 2) of the Office Action. Paragraph 4 simply quotes the statutory section. Paragraph 5 states that claim 12 is “generally narrative and indefinite, failing to conform with U.S. practice.” No portion of the claim has been identified in the Office Action in support of the holding of indefiniteness.

The second paragraph of 35 U.S.C. § 112 requires a claim to particularly point out and distinctly claim the subject matter considered to be the invention. Claims must be interpreted through the eyes of one having ordinary skill in the art in light of and consistent with the supporting specification. *Miles Laboratories, Inc. v. Shandon, Inc.*, 997 F.2d 870, 27 USPQ2d 1123 (Fed. Cir. 1993). Reasonable precision in light of the particular subject matter involved is all that is required by the second paragraph of 35 U.S.C. § 112. *Miles Laboratories, Inc. v. Shandon, Inc.*, 997 F.2d 870, 27 USPQ2d 1123 (Fed. Cir. 1993); *North American Vaccine, Inc. v. American Cyanamid Co.*, 7 F.3d 1571, 28 USPQ2d 1333 (Fed. Cir. 1993); *U.S. v. Telectronics Inc.*, 857 F.2d 778, 8 USPQ2d 1217 (Fed. Cir. 1988); *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 231 USPQ 81 (Fed.

Cir. 1986). For a tenable rejection under this section of the statute, the Office Action must provide a basis in fact and/or cogent technical reasoning to support the ultimate legal conclusion that one having ordinary skill in the art, with the supporting specification in hand, would not be able to reasonably ascertain the scope or protection defined by a claim. *In re Okuzawa*, 537 F.2d 545, 190 USPQ 464 (CCPA 1976).

Although the Office Action is accurate in stating that the controlling statutory section requires that a claim particularly point out and distinctly claim the subject matter which applicant regards as the invention, there is nothing in the statute that defines what is “narrative.” The Office Action does not define the term “narrative” nor explain what the Examiner finds to be deficient in the application of this term to the claimed recitation. Claim 12 is dependent from parent claim 11, a method (process) claim directed to a statutory category of invention. Under so-called “U.S. practice,” a method claim recites, or narrates, functions performed by the method steps.

Parent claim 11 has not been rejected under 35 U.S.C. § 112. Claim 12 further defines the step in claim 11 of generating, by the registration authority, a certificate issuing request. That is, claim 12 recites that the contents signed by the registration authority is a predetermined identifier to specify information to be certified by the public key certificate of the end entity. It is submitted that the recitation of claim 12 contains terms of art well understood by a person of ordinary skill in the art of encryption. The Office Action has presented no explanation, nor has identified any recitation of claim 12, that supports a conclusion that a person of ordinary skill in the art would not have understood what subject matter applicant regards as invention.

B. The rejection of claims 11 through 20 under 35 U.S.C. § 102(e) for anticipation by Matsuyama.

The factual determination of lack of novelty under 35 U.S.C. § 102 requires the identical disclosure in a single reference of each element of a claimed invention, such that the identically claimed invention is placed into the recognized possession of one having ordinary skill in the art. *Dayco Prods., Inc. v. Total Containment, Inc.*, 329 F.3d 1358, 66 USPQ2d 1801 (Fed. Cir. 2003); *Crown Operations International Ltd. v. Solutia Inc.*, 289 F.3d 1367, 62 USPQ2d 1917 (Fed. Cir. 2002). In imposing a rejection under 35 U.S.C. § 102, the Office Action must specifically identify wherein an applied reference is perceived to identically disclose each and every feature of a claimed invention. *In re Rijckaert*, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993); *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984). It is submitted that the Office Action does not meet the burden imposed in the above-identified precedents.

Claim 11, the only independent claim, reads as follows:

11. A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature certify contents that are to be included in the public key certificate, out of contents registered with the registration authority;

generating, by the registration authority, a certificate issuing request including the contents signed by the registration authority and the registration authority signature;

sending the certificate issuing request from the registration authority to the issuing authority; and

generating, by the issuing authority, the public key certificate including the contents signed by the registration authority, the registration authority signature, issuing contents issued by the issuing

authority, and an issuing authority signature signed by the issuing authority to certify the contents signed by the registration authority, the registration authority signature and issuing contents issued by the issuing authority.

Among other things, claim 11 requires that the public key certificate includes “contents signed by the registration authority and the registration authority signature.” Matsuyama, it is submitted, contains no such teaching.

The Office Action has read this claim requirement on the reference disclosure of Fig. 19, columns 22, 23. This portion of Matsuyama (column 23, lines 15, 16) refers to Figs. 6 and 7 for description of the public key certificate and its contents. There is nothing in either of those figures, nor in the description thereof in the specification, that indicates that the public key certificate is to contain contents signed by the registration authority and the registration authority signature.

The lack of such teaching by Matsuyama was emphasized to Examiner Doan in an interview conducted June 29, 2006. Examiner Doan directed attention to column 6, lines 47-57, asserting that this portion of the reference discloses the claim requirements at issue. This portion of Matsuyama is reproduced as follows:

In the public-key-encryption data-communication-system forming method, the public key certificate may include a common electronic signature of the public-key-certificate issuer authority which issues the public key certificate, and one of a root registration authority, a registration authority, a service provider, and a user device which perform processing for the verification of one public key certificate issued by the public-key-certificate issuer authority may perform offline processing for the verification of different public key certificates issued by a single public-key-certificate issuer authority.

It is submitted that this excerpt describes the contents of the public key certificate only to the extent that it may contain a common electronic signature of the public-key-certificate issuer authority which issues the public key certificate. The remaining portion of the excerpt is directed to identifying which elements may perform offline processing for the verification of different public key certificates

issued by a single public-key-certificate issuer authority. The recitation of root registration authority and registration authority in the excerpt are the latter elements that perform the processing function.

More specifically, the first portion of the excerpt that describes the contents of the public key certificate reads:

In the public-key-encryption data-communication-system forming method, the public key certificate may include a common electronic signature of the public-key-certificate issuer authority which issues the public key certificate, . . .

The next portion of the excerpt reads:

. . . and one of a root registration authority, a registration authority, a service provider, and a user device which perform processing for the verification of one public key certificate issued by the public-key-certificate issuer authority may perform offline processing for the verification of different public key certificates issued by a single public-key-certificate issuer authority.

Grammatically, the root registration authority, registration authority, service provider, and user device, in the second excerpted portion, serve as a subject clause for the verb action clause of performing processing for verification of the public key certificates. It is submitted that no person skilled in the art would find it conceivable that the public key certificate would contain one of the recited authorities. The authorities are entities that perform functions or generate data, and physically cannot be elements of a certificate. This position, it is submitted, is substantiated by the detailed examples of the public key certificate illustrated in Figs. 6 and 7, upon which the Office Action has relied.

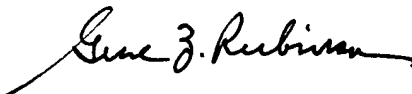
In summary, independent claim 11, and therefore claims 12 through 20 that depend therefrom, recite requirements that the public key certificate includes contents signed by the registration authority and the registration authority signature, requirements that Matsuyama does not disclose. It is therefore

10/076,624

submitted that the rejection of record, imposed under 35 U.S.C. § 102, is not legally viable. Reversal of the rejection is respectfully solicited.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

A handwritten signature in black ink, reading "Gene Z. Robinson". The signature is fluid and cursive, with a long horizontal stroke extending to the left.

Gene Z. Robinson
Registration No. 33,351

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 GZR:lnm
Facsimile: 202.756.8087
Date: September 28, 2006

**Please recognize our Customer No. 20277
as our correspondence address.**

VIII. CLAIMS APPENDIX

11. A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature certify contents that are to be included in the public key certificate, out of contents registered with the registration authority;

generating, by the registration authority, a certificate issuing request including the contents signed by the registration authority and the registration authority signature;

sending the certificate issuing request from the registration authority to the issuing authority;
and

generating, by the issuing authority, the public key certificate including the contents signed by the registration authority, the registration authority signature, issuing contents issued by the issuing authority, and an issuing authority signature signed by the issuing authority to certify the contents signed by the registration authority, the registration authority signature and issuing contents issued by the issuing authority.

12. A method as recited in claim 11, wherein
the contents signed by the registration authority is a predetermined identifier to specify information to be certified by the public key certificate of the end entity.

13. A method as recited in claim 11, wherein
the contents signed by the registration authority is a hash value calculated by applying a hash function to information to be certified by the public key certificate of the end entity.

14. A method for as recited in claim 11, further comprising the steps of:

verifying, by a verifying party, the issuing authority signature with the contents signed by the issuing authority; and

verifying, by the verifying party, the registration authority signature with the contents signed by the registration authority included in the public key certificate.

15. A method as recited in claim 12, further comprising the steps of:

acquiring, by a verifying party, information signed by the registration authority according to the identifier in the public key certificate;

calculating, by the verifying party, a hash value of the acquired information;

decoding, by the verifying party, the registration authority signature included in the public key certificate, by using a public key of the registration authority; and

checking by the verifying party, whether the hash value is identical to the decoded value.

16. A method as recited in claim 13, further comprising the steps of:

calculating, by a verifying party, a hash value of the information signed by the registration authority in the public key certificate;

decoding, by the verifying party, the registration authority signature included in the public key certificate, by using a public key of the registration authority; and

checking by the verifying party, whether the hash value is identical to the decoded value.

17. A method as recited in claim 14, further comprising the steps of:

constructing and verifying, by the verifying party, a path from the certificate authority trusted by the verifying party, up to the public key certificate;

verifying, by the verifying party, the registration authority signature described in the public key certificate using the public key of the registration authority; and

constructing and verifying, by the verifying party, a path from the certificate authority trusted by the verifying party up to the public key certificate of the registration authority.

18. A method as recited in claim 17; wherein

the verifying party obtains the public key certificate of the registration authority from a public key certificate database of the issuing authority according to the registration authority name described on the public key certificate.

19. A method as recited in claim 17; wherein

the verifying party obtains the public key certificate of the registration authority described in an extended region of the public key certificate to be verified.

20. As method as recited in claim 11, further comprising the steps of:

sending, by the registration authority, a certificate invalidation request to the issuing authority of the public key certificate of the registration authority;

receiving, by the issuing authority, the certificate invalidation request; and

invalidating, by the issuing authority, the public key certificate of the registration authority.

IX. EVIDENCE APPENDIX

No evidence has been submitted of record under 37 CFR 1.130, 1.131 or 1.132.

X. RELATED PROCEEDINGS APPENDIX

No decisions have been rendered in Related Appeals or Interferences.